[Insert Cover Picture]

Chemical Sector Civil Unrest Tabletop Exercise

Situation Manual

[Insert Date]

**\*[Insert Caveat]\***

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

This page is intentionally left blank.

# Exercise Agenda

| Start Time | End Time | Activity |
| --- | --- | --- |
| 8:00 a.m. | 8:30 a.m. | Registration |
| 8:30 a.m. | 8:45 a.m. | Welcome and Participant Briefing |
| 8:45 a.m. | 9:00 a.m. | Objectives |
| 9:00 a.m. | 9:45 a.m. | Module One: Information Sharing |
| 9:45 a.m. | 10:00 a.m. | Break |
| 10:00 a.m. | 10:45 a.m. | Module Two: Incident |
| 10:45 a.m. | 11:00 a.m. | Break |
| 11:00 a.m. | 11:45 a.m. | Module Three: Response and Recovery |
| 11:45 a.m. | 12:30 p.m. | Hot Wash and Closing Remarks |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Chemical Sector Civil Unrest Tabletop Exercise (TTX) |
| **Exercise Dates** | [Indicate the start and end dates of the exercise] |
| **Scope** | This exercise is a TTX planned for [insert exercise duration] at [insert exercise location]. Exercise play is limited to [insert exercise parameters].This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP). |
| **Mission Area(s)** | Prevention, Protection, Mitigation, Response, and Recovery [Select applicable Mission Areas] |
| **Capabilities** | * Economic Recovery
* Health and Social Services
* Intelligence and Information Sharing
* Operational Communication
* Operational Coordination
* Planning
* Public Information and Warning
* Risk Management for Protection Programs and Activities
* Situational Assessment
* [Insert additional core capabilities, as necessary]
 |
| **Objectives** | 1. Review intelligence and information sharing processes for a security incident with local or regional chemical sector critical infrastructure owners / operators.
2. Discuss private sector stakeholders’ emergency preparedness plans and response procedures to a security-initiated incident and the coordination activities under National Incident Management System (NIMS) with local, state, and federal agencies.
3. Examine recovery and business continuity plans and procedures following a security incident at a chemical facility.
4. [Insert additional exercise objectives, as necessary]
 |
| **Threat or Hazard** | Potential Civil Unrest [Insert additional threat vector, as necessary] |
| **Scenario** | A protest that turns violent disrupts a chemical facility.  |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being used, if applicable] |
| **Participating Organizations** | [Please see Appendix A.] |
| **Point of Contact** | [Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (POC) (e.g., exercise director or exercise sponsor).] |

# General Information

## Exercise Objectives and Capabilities

The exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

For additional information regarding capabilities, please visit:

<https://www.fema.gov/emergency-managers/national-preparedness/mission-core-capabilities>.

| **Exercise Objectives** | **Capability** |
| --- | --- |
| Review intelligence and information sharing processes for a security incident with local or regional chemical sector critical infrastructure owners / operators. | * Intelligence and Information Sharing
* Planning
* Public Information and Warning
 |
| Discuss private sector stakeholders’ emergency preparedness plans and response procedures to a security-initiated incident and the coordination activities under NIMS with local, state, and federal agencies. | * Operational Communication
* Operational Coordination
* Planning
* Public Information and Warning
* Risk Management for Protection Programs and Activities
* Situational Assessment
 |
| Examine recovery and business continuity plans and procedures following a security incident at a chemical facility. | * Economic Recovery
* Health and Social Services
* Operational Coordination
* Planning
 |
| [Insert additional objectives, as necessary] | * [Insert additional capabilities as necessary]
 |

Table 1. Exercise Objectives and Associated Capabilities

## Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

* **Players:** Players are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
* **Observers:** Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
* **Facilitator:** The facilitator provides situation updates and moderates discussions. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
* **Moderators:** Moderators are responsible for admitting and signing in all participants to the virtual exercise, monitoring the chat area for questions and / or issues, and controlling participant audio.
* **Evaluators:** Evaluators are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

## Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following three modules:

* Module One: Information Sharing
* Module Two: Incident
* Module Three: Response and Recovery

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate [insert mission area] issues.

## Exercise Guidelines

* This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
* Decisions are not precedent setting and may not reflect your jurisdiction’s / organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
* Issue identification is not as valuable as suggestions and recommended actions that could improve [insert mission area] efforts. Problem-solving efforts should be the focus.
* The assumption is that the exercise scenario is plausible, and events occur as they are presented. All players will receive information at the same time.

## Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and evaluator notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

# Module One: Information Sharing

## Scenario

### Location: [Insert Facility Name and Location]

### [Insert Month, Day, Year]: [Time]

An organized protest is set to take place throughout [insert location] in the upcoming days. According to the filed public gathering request, the main roads that the protest will occupy will be close to many businesses, including [insert chemical facility name].

While the organizers of the planned protest stressed that it will be a peaceful demonstration and condemn violence of all forms, the event has caught the attention of some opposing groups on various online forums, including opposing groups that have been known to incite or enact violence to further their own agendas.

Following the attention from these opposing groups, there has been a significant uptick in the number of individuals online and social media accounts that have posted alarming messages about the protest. Several of the posts call for individuals to rally at [insert location near facility] on the day of the protest to ‘counter’ the planned protest. Many commenters on these posts state they will show up armed.

Law enforcement noticed one such social media post, which has been shared heavily online amongst known members of opposing organizations, stating, “We will make sure these people get what’s coming to them, just like we did last month.” Included in the post is a picture from a previous demonstration that had ended in a violent altercation between opposing factions resulting in the grievous injuries of several people.

## Discussion Questions

1. How does your facility triage the information you receive (formal reporting, hearsay, and social media)?
2. What plans exist to prevent or deter an attack at your facility?
	1. What threats are you most concerned with preventing?
	2. Who is responsible for the security plan and necessary updates?
	3. Are multiple agencies outside of your organization involved in the response and recovery planning process?
3. How would your facility expect to receive information about a credible threat?
4. What steps does your facility take once they receive notice of a credible threat?
5. Does your facility conduct any specific training based on credible threats?
6. What formal information sharing processes would your facility use at this point?
7. What resources do you use to disseminate information?
	1. What notification capabilities (e.g., alerts, emails, telecom, text messages, special tools) do you use to share information and communicate the implementation of protective measures?
8. What measures would local law enforcement take at this time to protect your facility (e.g., outreach, increased patrols)?
9. How is your facility coordinating with information sharing partners (e.g. local law enforcement, Joint Terrorism Task Force [JTTF], fusion centers, etc.)?
10. Who is responsible for coordinating the risk communications message for your facility?
11. What are the key messages that your organization should distribute concerning the continuing credible threat to your facility and stakeholders?
	1. Do you coordinate the message with emergency services?
	2. If so, what is the process for coordinating this message?
12. What security recommendations, if any, are local, state, and federal law enforcement agencies making to private sector stakeholders at this time?
13. What additional actions are local, state, and federal law enforcement agencies taking at this point?
14. Are there additional notifications that you need to make outside of your organization?
15. What changes in the security posture at your facility would you implement in preparation for the demonstration date?

# Module Two: Incident

## Scenario

**Location:** **[Insert Facility Name and Location]**

### [Insert Month, Day, Year]: [Time]

[Insert your facility name] is engaged as usual in daily operations. Facility security staff notice a large crowd of people congregating outside the fence line and approaching the [insert your facility name] main gateway entrance. As the crowd moves closer, it becomes clear that the group is part of an organized protest; demonstrators are carrying picket signs with several leading chants with bullhorns. Based on the picket signs and chants, the protest appears to be separate from the previously anticipated demonstration that was planned. The crowd comes to a halt just a few hundred feet away from the main entrance.

Facility security staff respond to the main gate entrance and notify local law enforcement of the disturbance. The demonstration continues and most of the crowd continues to peacefully protest. Suddenly a small cohesive group, who all appear to be wearing the same kind of face coverings, break off from the main portion of the demonstration and begin pushing closer to the main gate. Security guards instruct the group to back away from the entrance and to move off the private property, but the masked individuals ignore their instructions and continue to push toward the security gate checkpoint office.

As the masked group advances towards the security staff, several individuals turn violent. Demonstrators launch personal items at the main entrance and security staff. One of the items thrown is a Molotov cocktail that explodes upon impact at the front of the guardhouse and entrance of the facility. Security guards and protesters alike begin running in all directions in response, with several individuals injured in the process. During the chaos, security personnel spot several individuals breaching the security perimeter and interacting with intake pipes to your facility.

## Discussion Questions

1. What plans exist to deter / prevent an unauthorized intrusion or attack (i.e., barricades, traffic control)?
2. What is the general security posture for your facility?
	1. What training programs exist for personnel? Are there specific training programs because of the hazardous nature of the materials used in your facility?
	2. How does your organization train personnel to respond to an unauthorized intrusion and a weaponized attack?
	3. What cross-training occurs between your facility’s security personnel and local first responders?
3. Do the organization’s standard operating procedures (SOPs) include incident response roles and responsibilities for staff?
	1. What specific procedures exist for the hazardous materials (HAZMAT) in your facility?
4. What assets are on-site to immediately respond to an incident?
	1. What resources are available that would help with response?
	2. What HAZMAT response training does your organization conduct for on-site response assets?
5. What additional off-site capabilities are available to respond to your facility?
	1. What HAZMAT assets are available to respond?
	2. What law enforcement assets are available to respond?
	3. What emergency medical services (EMS) assets are available to respond?
	4. Is there a local emergency management office that you would coordinate with?
6. What notification methods does your facility use to send alert information?
	1. Who is responsible for sending out the alerts or warnings?
	2. Have you pre-built message templates for different incidents?
	3. What protocols exist for alerting employees to an incident?
	4. What protocols exist for notifying authorities to the incident? How do you notify any first responders?
	5. What protocols exist for alerting partner organizations to an incident?
	6. What secondary alerting methods are available if the incident overloads the cell networks?
	7. What information is your organization releasing to the public at this time?
		1. How are you releasing this information?
		2. Who is responsible for the release of this information?
7. Does your facility conduct an accountability checks of your employees?
8. Would your organization enact crowd control and / or evacuation procedures?
	1. Who is responsible for activating the evacuation procedures or sheltering in place?
	2. How does your organization determine the preferred response between evacuating or sheltering in place?
	3. What procedures exist to secure critical areas and equipment if an immediate evacuation is required?
	4. Have you specified a location for evacuees? Are there secondary or tertiary rally points in case the primary location is part of the security incident?
	5. Who gives the all clear notification?
9. Has your organization pre-arranged agreements with any public or private sector organizations to provide resources? Are they formal or informal?
	1. How do you activate these agreements (i.e., what type of coordination and information sharing processes do the agreements require)?
	2. How will this coordination and information sharing take place?
10. What type of command structure would the responders establish?
	1. Who would be in charge?
	2. At what point would responders stand up an emergency operations center (EOC)?
		1. What agencies would be in the EOC?
	3. What is the role of private sector stakeholders in this command structure?
		1. Have they trained on incident command procedures?
	4. Who is in charge of securing the scene?

This page is intentionally left blank.

# Module Three: Response and Recovery

## Scenario

**Location:** **[Insert Facility Name and Location]**

### [Insert Month, Day, Year]: [Time + 20 Minutes]

The peaceful group of protesters disperses upon the situation turning violent. Officers responding to the scene quickly secure the area, begin to control the situation, and initiate mutual aid requests for fire and EMS response. The incident and ensuing panic left [insert number] individuals injured, including several facility security guards. The individuals interacting with the intake pipes dispersed with the rest of the crowd, and it is not presently clear if they caused any damage to the pipes.

As EMS arrives and treats the wounded, uninjured guards start to take account of the facility and property damage. The fire from the Molotov cocktail significantly damaged the security gate checkpoint office and caused minor damage to the front entrance of the facility after spreading there. Because of a prescheduled shift change at [insert your facility], several employees are filing in and out of the operational buildings and beginning to contact family members.

Law enforcement officials are continuing their investigation and have identified several suspects responsible for inciting violence. Social media begins to run rampant with rumors and speculations about the incident. Some claim that shots were fired in the chaos. Media outlets are beginning to arrive on scene and attempting to interview employees and first responders.

## Discussion Questions

1. What training does personnel undergo to assess potential damage to process equipment, storage tanks, or pipelines running through or into the facility for potential chemical leaks?
2. How would non-essential workers leave the facility if the chaos blocked or damaged the roads?
	1. How would first responders / HAZMAT response gain access to the facility?
3. Does your organization have a continuity of operations / business plan?
	1. Does it include a crisis communications plan?
		1. How and what type of messaging will your organization send to employees, vendors, and customers?
		2. What training do employees receive regarding media relations and the release of sensitive information?
	2. What are the short-term recovery objectives for your facility?
	3. What are the implications of being unable to open or operate for a period of time?
		1. Given the scenario, how long would the incident area remain cordoned off for the investigation?
		2. What would the financial impact be on your facility if such an incident and the ensuing investigation closed a building?
		3. Would there be any supply chain issues and / or interdependencies with other companies that could have national or international impacts?
	4. Can your facility move key operations to another location?
		1. If so, how long would this take?
	5. Do you have any insurance that would assist given this scenario?
		1. If [insert appropriate organization] had declared the incident terrorism, would this impact insurance?
	6. What training plans exist for the business continuity plan? Does your organization exercise these plans (other than today)?
4. What communication methods does your facility and other private sector organizations use to share information?
	1. How do you communicate with first responders?
	2. What other private sector organizations would you communicate with?
	3. What communication methods would you use for coordinating with your private sector partners?
	4. Who in your organization is responsible for communication during an incident?
	5. What alternate communication procedures exist?
5. What communication methods do first responders use to share information with other responders?
	1. How do multiple on-scene response agencies from multiple jurisdictions coordinate communications? Who is in charge of this?
	2. How do you communicate with private sector response resources?
	3. What secondary communications capabilities exist in case primary systems fail?
		1. What information do you communicate to the public?
6. How can facility owners / operators prepare to handle the public messaging / media in the aftermath of such an incident?
	1. What messaging does your organization send out to the media about the current situation?
	2. What and how does your organization convey information to the public at this time?
	3. How will you restore public confidence?
	4. How will you resolve potential misinformation?
	5. Is your organization monitoring social media to maintain awareness of information spreading that may not be accurate?
		1. Who is responsible for this?
		2. What procedures exist to counter false information on social media?
7. Given the scenario, what measures would your organization need to support your employees or other persons at your facility following this event?
	1. How do you communicate this information to employees during the days following the incident?
	2. If you must suspend operations for a length of time, is there financial assistance available to employees?
	3. Are there any additional security measures that you would put into place following this event?
	4. How do you reassure employees as to their safety on the job?
8. What resources are available to assist your facility with recovery?
	1. Have you pre-arranged agreements with other organizations to obtain key resources?
	2. If so, how does your organization activate these agreements (i.e., what type of coordination and request processes do the agreements require)?
	3. Would your organization or state / local organizations be requesting grant assistant to support recovery efforts?
9. What are your facility’s interdependencies?
	1. What stakeholders are dependent upon your facility and its services?
	2. Who are the key stakeholders or groups that your facility relies upon to help restore your operations and assets?
	3. What public sector organizations / resources does your facility rely on to help restore critical infrastructure assets?
	4. Do you have contracts / agreements in place with the organizations that control / own these resources / services for priority services in an emergency?
	5. Who are the key mobilizers or champions (either individuals or functional roles) in your organization or community who you must engage for an effective recovery?
10. What public communications or warnings is your organization disseminating?
11. Who would make decisions regarding the release of information to the public?
12. How quickly is your organization releasing information?
13. What methods are you using to distribute information?
14. How do the relevant stakeholders coordinate public messaging?
15. What measures does your organization take to disrupt the distribution of fake information?
16. What is the process to collect evidence that belongs to citizens (cell phone video, cameras, security footage from private businesses, etc.)?
17. How do you reunite owners with their personal items left at the scene?

# Appendix A: Exercise Participants

| **Participating Private Sector Organizations** |
| --- |
| [Insert private sector participants] |
|  |
|  |
|  |

| **Participating Local Organizations** |
| --- |
| [Insert local participants] |
|  |
|  |
|  |

| **Participating State Organizations** |
| --- |
| [Insert state participants] |
|  |
|  |
|  |

| **Participating Federal Organizations** |
| --- |
| [Insert federal participants] |
|  |
|  |
|  |

| **Other Participating Organizations** |
| --- |
| [Insert other participants] |
|  |
|  |
|  |

This page is intentionally left blank.

# Appendix B: Relevant Plans

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

# Appendix C: Acronyms

| Acronym | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP** | CISA Tabletop Exercise Package |
| **EMS** | Emergency Medical Services |
| **EOC** | Emergency Operations Center |
| **EPT** | Exercise Planning Team |
| **HAZMAT** | Hazardous Materials |
| **IP** | Improvement Plan |
| **JTTF** | Joint Terrorism Task Force |
| **NIMS** | National Incident Management System |
| **POC** | Point of Contact |
| **SitMan** | Situation Manual  |
| **SME** | Subject Matter Expert |
| **SOP** | Standard Operating Procedures |
| **TTX** | Tabletop Exercise  |

